IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA
MINNEAPOLIS DIVISION

Robert Taylor, individually and on behalf all others similarly situated, Plaintiff, v. Fortra, LLC, Defendant.	**CASE NO._____** **CLASS ACTION** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

1. Plaintiff Robert Taylor ("Plaintiff") brings this action on behalf of themselves and all others similarly situated against Defendant Fortra, LLC (formerly known as Help/Systems, LLC) ("Fortra" or "Defendant"). Plaintiff seeks to obtain damages, restitution, and injunctive relief for a class of individuals ("Class" or "Class Members") who are similarly situated and have received notices of the data breach from customers of Defendant Fortra, a cybersecurity and automation information technology software company. These third-party entities include Hatch Bank and other companies or organizations who are Fortra's customers ("Customers"), which have been attacked by cybercriminals as a result of Fortra's negligence.

2. Plaintiff makes the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record.

I. NATURE OF THE ACTION

3. This class action arises out of a massive January 2023 data breach ("Data Breach") of documents and information stored on the computer network of Fortra, including but not limited to Fortra's "GoAnywhere" site.[1]

4. On its computer network, Fortra holds and stores certain highly sensitive personally identifiable information ("Private Information") on behalf of various businesses to which it provides its services (*i.e.*, Forta's Customers), including for example Hatch Bank. Customers collect the Private Information of Plaintiff and Class Members, i.e., individuals who provided their highly sensitive and confidential personal information in exchange for business services offered by the Customers. The Customers then entrust Fortra to organize, store, and protect that Private Information on their behalf.

5. According to the Notice of Data Breach Letter that Hatch Bank sent to Plaintiff and Class Members related to its business, Fortra first became aware of "a vulnerability located in their software" on or about January 29, 2023 and began investigating.[2]

6. Fortra's investigation determined that there was a breach to its computer network from January 30, 2023, to January 31, 2023. On or about February 3, 2023, Fortra notified Hatch Bank (and upon information and belief, other Customers) of the incident. It informed Hatch Bank that the files it stored for Hatch Bank on Fortra's GoAnywhere site

[1] *See* Notice of Data Event located at: https://apps.web.maine.gov/online/aeviewer/ME/40/4cfbf86f-8d04-4296-9195-81b874ba939a.shtml (last accessed on March 2, 2023).
[2] See Exhibit A, Plaintiff's Notice Letter.

were subject to unauthorized access.

7. Similarly, according to a February 13, 2023 Securities and Exchange Commission K-8 filing by Community Health Systems, Inc. ("CHS"), another Customer of Fortra, LLC, it was similarly notified "that Fortra had experienced a security incident that resulted in the unauthorized disclosure of [CHS] data" through its secure file transfer software, GoAnywhere. As a result of this breach, both Protected Health Information ("PHI") and "Personal Information" ("PI") of approximately one million CHS patients were exposed.[3]

8. Hatch Bank began notifying the approximately 139,493 consumers associated with its banking business on or about February 28, 2023, approximately a month after the data breach occurred, stating that their personally identifying information had been stolen in what Defendants call a "security incident."[4]

9. Customers' (including Hatch Bank, CHS, and others) reliance on Fortra's technology led to unauthorized access to hundreds of thousands of individuals' names and Social Security numbers as well as Personally Identifying Information ("PII") and Protected Health Information ("PHI") depending on the Customer's specific business type. The victims of Fortra's data breach include Plaintiff and Class Members.[5]

10. As a result of Defendant's Data Breach subjecting Customers' data to unauthorized access and exfiltration, Plaintiff and hundreds of thousands (if not more) of

[3] https://www.sec.gov/Archives/edgar/data/1108109/000119312523035789/d422693d8k.htm (last accessed March 6, 2023).
[4] *See* Exhibit A.
[5] *Id.*

Class Members suffered ascertainable losses in the form of invasion of privacy and financial losses resulting from identity theft, out-of-pocket expenses, the loss of the benefit of their bargain, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

11. Plaintiff's and Class Members' highly sensitive personal information—which was entrusted to Defendant by its Customers was compromised and unlawfully accessed and extracted during the Data Breach.

12. Based upon Hatch Bank's website notification and its notice letter, as well as CHS's SEC filing quoted above, the Private Information compromised in the Data Breach was intentionally accessed and removed, also called exfiltrated, by the cyber-criminals who perpetrated this attack and remains in the hands of those cyber-criminals.

13. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Plaintiff and Class Members' Private Information, despite selling its software and data protection services to Customers for that very purpose.

14. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that was collected by Customers and maintained by Defendant, and for failing to provide timely and adequate notice of its "software vulnerabilities" to Customers so they might mitigate and prevent the Data Breach, and so that information could be transmitted to Plaintiff and other Class Members to prevent or reduce the injuries resulting from their Private Information being stolen by cybercriminals.

15. Defendant maintained its software and the stored Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks. The mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a well-known risk to Defendant. Thus, Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

16. Defendant disregarded the privacy and property rights of Plaintiff and Class Members by, inter alia, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard Plaintiff's and Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff and Class Members prompt and accurate and complete notice of the Data Breach.

17. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant properly monitored its computers, it would have discovered the software vulnerability and risk of criminal intrusion sooner and been able to mitigate the injuries to Plaintiff and the Class.

18. Plaintiff's and Class Members' identities are now at substantial and imminent risk because of Defendant's negligent conduct since the Private Information that

Defendant collected and maintained (including Social Security numbers) is now in the hands of data thieves.

19. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

20. Plaintiff and Class Members may also incur, or have already incurred, out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

21. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of themselves and a Class (defined below) of all similarly situated individuals whose Private Information was accessed during the Data Breach.

22. Accordingly, Plaintiff brings this action against Defendant for negligence, breach of implied contract, unjust enrichment, and declaratory relief, seeking redress for Defendant's unlawful conduct.

23. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate, long term credit monitoring services funded by Defendant, and declaratory relief.

II. PARTIES

24. Plaintiff Robert Taylor is and at all times relevant to this Complaint an individual citizen of the State of Connecticut, residing in the city of New London (New

London County). Plaintiff Taylor received a Notice of the Data Breach from Hatch Bank, a Customer of Defendant Fortra. A copy of the notice he received is dated February 28, 2023 and attached as Exhibit A (the "Notice Letter").

25. Defendant Fortra, LLC, is a limited liability company organized and registered according to the laws of the State of Delaware. Defendant Fortra maintains its primary headquarters in Eden Prairie, Minnesota. Fortra's principal place of business is located at 11095 Viking Drive, Suite 100, Eden Prairie, Minnesota, 55344.

26. Plaintiff reserves the right to seek leave to add other necessary defendants responsible for Plaintiff's and Class Members' damages and injuries, including but not limited to any parent company, principals, members, or affiliate of Fortra and/or its Customers, including but not limited to Hatch Bank.

III. JURISDICTION AND VENUE

27. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

28. The Court has general personal jurisdiction over Defendant because, personally or through its agents, Defendant operates, conducts, engages in, or carries on a business or business venture in this State; it is registered with the Secretary of State of Minnesota as a for-profit limited liability company; it maintains its headquarters in Minnesota; and committed tortious acts in Minnesota.

29. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because it is the district within which Defendant has the most significant contacts.

IV. STATEMENT OF FACTS

Nature of Defendant's Business.

30. Fortra is a company that provides cybersecurity services to its Customers, including Hatch Bank, in the forms of: data monitoring, storage and reporting, security recommendations, risk assessments, etc.[6]

31. Fortra has five headquarters worldwide, located in: the United States, United Kingdom, Spain, Argentina, and Australia.[7]

32. Fortra promises its customers to protect their sensitive data through their cybersecurity services. Fortra claims it, "delivers a layered data security defense for your most sensitive data."[8]

33. Fortra understands the importance of having a well-protected computer network guarding against cybercriminals. In fact, it offers "offensive security" services "to be a deterrent, providing significant obstacles to ensure that attackers never see your environment as an easy target, but instead one that would be time consuming, labor intensive, and ultimately not worth the hassle."[9]

34. It also offers vulnerability management, email security, anti-phishing, digital risk protection, secure file transfer, and data protection along with its other "offensive

[6] https://www.fortra.com/services/managed-services (last accessed March 3, 2023).
[7] https://www.fortra.com/contact-us (last accessed March 3, 2023).
[8] https://www.fortra.com/solutions#securityservices (last accessed March 3, 2023).
[9] https://www.fortra.com/solutions/data-security/offensive-security (last accessed March 3, 2023).

security" services.

35. Fortra advertises to its customers to "Let our cybersecurity experts help. We have the experience and resources to help you implement a multi-layered defense that protects your organization without disrupting business activity." [10]

36. Fortra collects and stores Plaintiff's and Class Members' PII (Personally Identifiable Information) and PHI (Protected Health Information) in its record-keeping systems on behalf of its Customers, including but not limited to Hatch Bank, who have collected this information from consumers or patients in exchange for their business services.

37. More specifically, Fortra receives sensitive PII from its Customers in industries like banking, including Hatch Bank for example, holding information such as Social Security numbers, banking and/or financial account information, names, birth dates, addresses, and government identification/driver's license numbers.

38. Upon information and belief, in the ordinary course of receiving medical records from Fortra's medical Customers, Fortra is provided with sensitive, personal PII and PHI including names, birth dates, medical record numbers, health insurance information, Social Security numbers, and medical care information.

39. Fortra publicly recognizes it has a duty to securely maintain Private Information from its customers and has published several news articles on the critical importance of data security, including "*The Last Watchdog: The Drivers Behind Persistent*

[10] https://www.fortra.com/solutions#securityservices (last accessed March 3, 2023).

Ransomware and Defensive Tactics to Deploy," "*SC Magazine: Reduce Risk By Redefining Security*," and "*Forbes Advisor: Hackers Want to Crack Your Smartphone. Here Are 8 Ways to Fight Back*."[11]

40. Fortra's news releases detail why companies that store Private Information have a duty to safeguard such information against theft and explain how to safeguard Private Information when they collect it.

41. In fact, in "*Over One Quarter of Organizations Have No Plans to Implement Cybersecurity Measures Despite Cybersecurity Remaining Top Concern*," Fortra advises Customers about the hazards of ignoring proactive cybersecurity measures: "Organizations that neglect to prioritize these security controls risk being brought to their knees by data breaches, ransomware, or other cyberattacks that prey on security vulnerabilities," assuring Customers that by choosing Fortra to defend it computer networks, Fortra will be "your relentless ally to provide peace of mind through every step of your cybersecurity journey."[12]

42. In a press release from Fortra, "*SC Magazine: Reduce Risk By Redefining Security,*" Fortra lists three "pillars" to focus on: (i) Visibility; (ii) Exposures; (iii) Threats, explained further as shown below:[13]

[11] https://www.fortra.com/resources?f%5B0%5D=type%3A1331 (last accessed March 6, 2023).
[12] https://www.fortra.com/resources/press-releases/over-one-quarter-organizations-have-no-plans-implement-cybersecurity (last accessed March 6, 2023).
[13] https://www.fortra.com/resources/press-releases/sc-magazine-reduce-risk-redefining-security (last accessed March 6, 2023).

- **Visibility.**

Security teams must have visibility into the battlespace. So, what kind of visibility does the organization have? Does the team know when a new asset gets spun up in AWS, Azure, or even in the data center? Do the security tools know about it? Are agents installed and are they properly configured? Is the team confident in how its perimeter devices are configured? What are the limitations in the organization's ability to prevent or detect threats in these environments? The team needs the right tools, in the right locations, configured correctly.

Lack of visibility is the biggest reason for missed attacks. To properly protect a network, the team must know where its visibility gaps are and build a plan to address them. Start by asking the customer if they know all the assets in their environment. Most of the time the response comes from a manually-managed spreadsheet.

- **Exposures.**

We need to understand where our weaknesses – our soft points – are in our battle position. When assessing exposures, it's natural to lean into vulnerabilities – such as out-of-date software – but there's more to uncover here. Understanding these exposures are important, but we must also account for the biggest risk. Think about this with the aid of threat modeling techniques. What am I most concerned about and what are the likely avenues of approach? Where are my weaknesses? When we're analyzing exposures, we're looking to better understand where our risks are. We're not just talking about out-of-date applications or services. We're also talking about misconfigurations, exposed S3 buckets, and overprivileged identity and access management roles. Gain a full understanding of the breadth of exposures and regularly monitor and report on them.

- **Threats.**

All organizations are under constant attack, relentlessly being probed from every direction. These threats are what the team prepares for and – based on how the organization is attacked – bring additional light to the team's assessment of the battlespace. But does the team know what types of attacks it's experiencing and what resources are under attack. All too often I see a business just absorb these attacks and brush off successfully-blocked attacks as the result of a tool doing its job, but the team must leverage this intelligence. How many controls were bypassed before antivirus picked up on the malware? Does the team know which assets take on the plethora of attacks? What types of attacks will the team experience? How well are the controls working? How can the team adjust because of these findings? Understanding how and where the team gets attacked is critical in helping it prioritize the work.

To effectively protect the organization on the digital battlefield, the team needs to first redefine its security posture by looking at the three VET pillars: Organizations can maintain a good security posture doing the following:

- Maintain constant visibility of newly deployed assets.
- Combine threats and exposures to properly prioritize patches.
- Prioritize architecture decisions that lead to increased visibility and reduced exposures.

By understanding these three pillars, the team can now make decisions and prioritize projects based on data rather than on a whim. These are decisions that will protect the organization against known and unknown attacks.

43. Moreover, Fortra understands the critical importance in protecting PHI specifically. In fact, Fortra informs medical Customers on HIPAA compliance and the consequences of noncompliance:[14]

Consequences of Not Complying with HIPAA

The need to share health data is there – by hospitals, clinics, insurers, research facilities, pharmacies, and public health organizations. However, very specific guidelines around how this information can be stored and shared are needed to ensure patient privacy. Breaching the trust of individuals who've entrusted their data comes with consequences.

[14] https://www.fortra.com/solutions/data-security/compliance/hipaa-compliance (last accessed March 6, 2023).

According to HIPAA security laws and regulations for professionals, the Office for Civil Rights (OCR) within the HSS is responsible for enforcing Privacy and Security Rules, establishing compliance requirements as well as for levying civil monetary penalties.

Organizations that fail to comply with HIPAA regulations can see substantial fines levied against them, even if no actual PHI breach occurs. In addition, criminal charges and even civil action lawsuits can be filed following a breach. And it should be noted: ignorance of HIPAA compliance requirements doesn't pass muster as a defense against violations sanctions. The OCR issues fines whether a violation is inadvertent or is the result of willful neglect.

Ensuring your administrative policies and procedures, physical protection, as well as technical solutions as a Covered Entity or Business Associate are in place can go a long way in keeping off the OCR's radar.

44. Furthermore, Fortra provides Customers with a HIPAA Security Rule Checklist with tips on how *not to risk* unauthorized disclosure of PHI and PII:[15]

HIPAA Security Rule Checklist

There are three categories of safeguards to help ensure the HIPAA Security Rule is adhered to by covered Entities and Business Associates – administrative, physical, and technical.

Administrative Safeguards to Meet HIPAA Security Rule Requirements

Identification and analysis
Identification and analysis of possible risks to e-PHI and placement of appropriate and reasonable security measures to reduce them.

Designate a security official
Designate a someone to be responsible for developing and implementing security policies and procedures.

Manage information access
Manage information access per Privacy and Security Rules. The Privacy Rule limits the use and disclosure of e-PHI to the "minimum necessary." The Security Rule requires role-based access policies and procedures for authorizing access to e-PHI.

[15] *Id.*

Training and management of workforce
Training and management of workforce on e-PHI policies and procedures. All workforce members must be training regarding a covered entity's security policies and procedures with appropriate sanctions for violations of them.

Evaluation of Policies and Procedures
Evaluation of Security Rule Policies and Procedures: Periodically, current policies and procedures should be reviewed for how well they meet the established HIPAA requirements.

45. Fortra was aware of its duties to protect the Private Information of Plaintiff and Class Members. Fortra misleads and deceives its Customers through its published articles, particularly those emphasizing data security. Even though Fortra claims that it "transformed the industry by bringing the leading solutions into one best-in-class portfolio, creating a stronger line of defense from a single provider," on information and belief, Fortra does not follow its own recommended, industry standard practices in securing PII and PHI.

The Data Breach.

46. According to the Notice of Data Breach Letter that Hatch Bank sent to Plaintiff and Class Members who had accounts at or were otherwise customers of this financial institution, Fortra first became aware of "a vulnerability located in their software" on or about January 29, 2023 and began investigating.

47. Fortra's investigation determined that there was a breach to its computer network from January 30, 2023, to January 31, 2023.

Customer Hatch Bank

48. On or about February 3, 2023, Fortra notified Hatch Bank of the incident and informed Hatch Bank that the files it stored on Fortra's GoAnywhere site were subject to

unauthorized access.

49. Hatch Bank began notifying the approximately 139,493 victims on or about February 28, 2023, approximately a month after the data breach occurred, stating that their PII had been stolen in what Defendants call a "security incident."

50. Hatch Bank's reliance on Fortra's technology led to unauthorized access to its customers' names and Social Security numbers, including those of Plaintiff and Class Members.

Other Fortra Customers

51. Upon information and belief, in early February 2023, Fortra also began notifying its other Customers, including CMS, of the Data Breach as well. It is uncertain if other Customers of Fortra have sent notice letters to their patients or clients as of the filing date of this Complaint, or if those Customers will be notifying their affected Class Members at a later date.

52. Similarly, other Fortra Customers' reliance on Fortra's technology led to unauthorized access to consumers' and patients' names and Social Security numbers, other PII and PHI, including those of other Class Members.

All Class Members

53. ***Plaintiff's and Class Members' PII is or may have been in the hands of cybercriminals for months before being notified*** of Defendant's Data Breach by the individual Customers of Fortra since each Customer is separately notifying its clients, consumers and patients. Time is of the essence when trying to protect against identity theft after a data breach, so comprehensive and efficient notification to victims is critical, yet is

not occurring here.

54. Because of this targeted, intentional cyberattack, data thieves were able to gain access to and obtain data from Defendant that included the Private Information of Plaintiff and Class Members.

55. Upon information and belief, the Private Information stored on Defendant's network was not encrypted.

56. Plaintiff's and Class Members' Private Information was accessed and stolen in the Data Breach. Plaintiff reasonably believes the stolen Private Information is currently available for sale on the Dark Web because that is the *modus operandi* of cybercriminals who target businesses that collect highly sensitive Private Information.

57. As a result of the Data Breach, Defendant's Customers are now having to encourage Class Members to enroll in credit monitoring, fraud consultation, and identity theft restoration services, a tacit admission of the imminent risk of identity theft faced by Plaintiff and Class members.[16]

58. That Defendant, through its Customers, is encouraging Plaintiff and Class Members to enroll in credit monitoring and identity theft restoration services is an acknowledgment that the impacted consumers are subject to a substantial and imminent threat of fraud and identity theft.

59. Defendant had obligations created by contract, industry standards, and common law to keep Plaintiff's and Class Members' Private Information confidential and

[16] Notice Letter, Exhibit A.

to protect it from unauthorized access and disclosure.

60. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing PII.

Defendant Acquires, Collects, and Stores Private Information.

61. Defendant acquires, collects, and stores a massive amount of personally identifiable information ("PII") of consumers for its Customers.

62. By obtaining, collecting, and using Plaintiff's and Class Members' PII for its own financial gain and business purposes, Defendant assumed legal and equitable duties and knew that it was responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure.

63. Plaintiff and the Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

64. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

The Data Breach was a
Foreseeable Risk of which Defendant was on Notice

65. It is well known that PHI and PII, including Social Security numbers in particular, are valuable commodities and a frequent, intentional target of cyber criminals. Companies that collect such information, including Defendant, are well aware of the risk of being targeted by cybercriminals.

66. Individuals place a high value not only on their PII, but also on the privacy of that data. Identity theft causes severe negative consequences to its victims, as well as severe distress and hours of lost time trying to fight against the impact of identity theft.

67. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice, "[a] direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss."[17]

68. Individuals, like Plaintiff and Class members, are particularly concerned with protecting the privacy of their Social Security numbers, which are the key to stealing any person's identity and is likened to accessing your DNA for hacker's purposes.

69. Data Breach victims suffer long-term consequences when their Social Security numbers are taken and used by hackers. Even if they know their Social Security numbers are being misused, Plaintiff and Class Members cannot obtain new numbers unless they become a victim of social security number misuse.

[17] "Victims of Identity Theft, 2018," U.S. Department of Justice (April 2021, NCJ 256085) available at: https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed March 3, 2023).

70. The Social Security Administration has warned that "a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same."[18]

71. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[19]

72. Additionally in 2021, there was a 15.1% increase in cyberattacks and data breaches since 2020. Over the next two years, in a poll done on security executives, they have predicted an increase in attacks from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable causes will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[20]

73. In light of high profile data breaches at other companies, including Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January

[18] https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed March 3, 2023).
[19] https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last accessed March 3, 2023).
[20] https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864 (last accessed March 3, 2023).

2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that its computer network would be targeted by cybercriminals.

74. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, and hopefully can ward off a cyberattack.

75. According to an FBI publication, "[r]ansomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data." [21] This publication also explains that "[t]he FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity."[22]

76. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII private and secure, Defendant failed to take appropriate steps to protect the PII of Plaintiff and the proposed Class from being compromised.

[21] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware (last accessed March 3, 2023).
[22] *Id.*

At All Relevant Times Defendant Had a Duty to Properly Secure PII

77. At all relevant times, Defendant had a duty to Plaintiff and Class Members to properly secure their PII and PHI, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff and Class Members, and to promptly notify Plaintiff and Class Members when Defendant became aware that their PII was compromised.

78. Defendant had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, Defendant breached its common law, statutory, and other duties owed to Plaintiff and Class Members.

79. Security standards commonly accepted among businesses that store PII and PHI using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

80. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[23] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[24]

81. The ramifications of Defendant's failure to keep consumers' PII secure are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims including Plaintiff and the Class may continue for years.

The Value of Personal Identifiable Information

82. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200.[25]

[23] 17 C.F.R. § 248.201 (2013).
[24] *Id.*
[25] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed March 3, 2023).

83. Criminals can also purchase access to entire company's data breaches from $900 to $4,500.[26]

84. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[27]

85. Attempting to change or cancel a stolen Social Security number is difficult if not nearly impossible. An individual cannot obtain a new Social Security number without evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

86. Even a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all

[26] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/(last accessed March 3, 2023).
[27] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed March 3, 2023).

of that old bad information is quickly inherited into the new Social Security number."[28]

87. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[29]

88. PII can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[30]

89. Given the nature of this Data Breach, it is foreseeable that the compromised PII can be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Class Members' PII can easily obtain Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

90. The Private Information compromised in this Data Breach is static and difficult, if not impossible, to change (such as Social Security numbers).

91. Moreover, Hatch Bank has offered only a limited 1-year subscription for identity theft monitoring and identity theft protection through Cyberscout. Its limitation is

---

[28] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed March 3, 2023).

[29] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed March 3, 2023).

[30] *See* OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1 (last accessed March 3, 2023).

inadequate when Defendant's victims are likely to face many years of identity theft.

92. Furthermore, Defendant and its Customers' credit monitoring offer and advice to Plaintiff and Class Members squarely places the burden on Plaintiff and Class Members, rather than on Defendant, to monitor and report suspicious activities to law enforcement. In other words, Defendant and its Customers expect Plaintiff and Class Members to protect themselves from its tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiff and Class Members in credit monitoring services upon discovery of the breach, Defendant merely sent instructions to Plaintiff and Class Members about actions they can affirmatively take to protect themselves.

93. These services are wholly inadequate as they fail to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud, and they entirely fail to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

94. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the victims of its Data Breach.

Defendant Failed to Comply with FTC Guidelines

95. Federal and State governments have established security standards and issued recommendations to mitigate the risk of data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security

practices. According to the FTC, the need for data security should be factored into all business decision-making.[31]

96. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[32] The guidelines note businesses should protect the personal consumer and consumer information that they keep, as well as properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

97. The FTC emphasizes that early notification to data breach victims reduces injuries: "If you quickly notify people that their personal information has been compromised, they can take steps to reduce the chance that their information will be misused" and "thieves who have stolen names and Social Security numbers can use that information not only to sign up for new accounts in the victim's name, but also to commit tax identity theft. People who are notified early can take steps to limit the damage."[33]

98. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[34]

---

[31] Federal Trade Commission, *Start With Security, available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed March 3, 2023).
[32] Federal Trade Commission, *Protecting Personal Information: A Guide for Business, available at*: https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last accessed March 3, 2023).
[33] https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business (last accessed March 3, 2023).
[34] *See* FTC, *Start With Security*, *supra*.

99. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks.

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall

separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

100. The FTC has brought enforcement actions against businesses for failing to protect consumer and consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security

obligations.

101. Because Class Members entrusted Customers of Defendant with their PII, Defendant had, and has, a duty to the Plaintiff and Class Members to keep their PII secure.

102. Plaintiff and the other Class Members reasonably expected that when they provide PII to Customers of Defendant, Defendant would safeguard their PII.

103. Defendant was at all times fully aware of its obligation to protect the personal and financial data of consumers, including Plaintiff and members of the Class. Defendant was also aware of the significant repercussions if it failed to do so. Its own news releases, quoted above, acknowledges this awareness.

104. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—including Plaintiff's and Class Members' first names, last names, addresses, and Social Security numbers, and other highly sensitive and confidential information—constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Class Members Have Suffered Concrete Injury as a Result of Defendant's Inadequate Security.

105. Plaintiff and Class Members reasonably expected that the Customers of Defendant would provide adequate security protections for their PII, and Class Members provided to Customers, who in turn trusted Defendant with sensitive personal information, including Plaintiff's and Class Members' names, addresses, and Social Security numbers, PHI, and PII in exchange for its services.

106. Defendant's poor data security deprived Plaintiff and Class Members of the

benefit of their bargain. Plaintiff and other individuals whose PII was entrusted with Defendant understood and expected that, as part of that business relationship, they would receive data security, when in fact Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received data security that was of a lesser value than what they reasonably expected. As such, Plaintiff and the Class Members suffered pecuniary injury.

107. Cybercriminals intentionally attack and exfiltrate PII to exploit it. Thus, Plaintiff and Class Members are now, and for the rest of their lives will be, at a heightened and substantial risk of identity theft. Plaintiff has also incurred (and will continue to incur) damages in the form of, inter alia, loss of privacy and costs of engaging adequate credit monitoring and identity theft protection services.

108. The cybercriminals who obtained the Plaintiff's and Class Members' PII and, in some cases, PHI, may exploit the information they obtained by selling the data in so-called "dark markets" or on the "dark web." Having obtained these names, addresses, Social Security numbers, and other PII, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member's name, including but not limited to:

- obtaining employment;
- obtaining a loan;
- applying for credit cards or spending money;
- filing false tax returns;
- stealing Social Security and other government benefits; and

- applying for a driver's license, birth certificate, or other public document.

109. In addition, if a Class Member's Social Security number is used to create false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the person's ability to gain employment or obtain a loan.

110. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiff and other Class Members have been deprived of the value of their PII, for which there is a well-established national and international market.

111. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for fraudulent misuse of this information to be detected.

112. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the other Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud. Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach." Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud."[35] Moreover, there is

[35] The Consumer Data Insecurity Report: Examining The Data Breach- Identity Fraud Paradigm In Four Major Metropolitan Areas, (*available at* https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf) (last accessed March 3, 2023).

a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members' PII will do so at a later date or re-sell it.

113. As a result of the Data Breach, Plaintiff and Class Members have already suffered injuries, and each are at risk of a substantial and imminent risk of future identity theft.

114. Defendant admits that the unknown actor gained access to the Defendant network and obtained certain data on its computer systems. In other words, Plaintiff reasonably assumes that cybercriminals actually exfiltrated the accessed PII.[36]

Data Breaches Put Consumers at an Increased Risk Of Fraud and Identify Theft

115. Data Breaches such as the one experienced Plaintiff and Class Members are especially problematic because of the disruption they cause to the overall daily lives of victims affected by the attack.

116. In 2019, the United States Government Accountability Office released a report addressing the steps consumers can take after a data breach.[37] Its appendix of steps consumers should consider, in extremely simplified terms, continues for five pages. In addition to explaining specific options and how they can help, one column of the chart explains the limitations of the consumers' options. *See* GAO chart of consumer

[36] See Notice Letter, Ex. A.
[37] https://www.gao.gov/assets/gao-19-230.pdf (last accessed March 3, 2023). *See* attached Ex. B.

recommendations, reproduced and attached as Exhibit B. It is clear from the GAO's recommendations that the steps Data Breach victims (like Plaintiff and Class Members) must take after a breach like Defendant's are both time consuming and of only limited and short-term effectiveness.

117. The GAO has long recognized that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record," discussing the same in a 2007 report as well ("2007 GAO Report").[38]

118. The FTC, like the GAO (see Exhibit B), recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[39]

119. Theft of Private Information is also gravely serious. PII and PHI is a valuable property right.[40]

120. It must also be noted there may be a substantial time lag – measured in years

---

[38] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last accessed March 3, 2023) ("2007 GAO Report").

[39] *See* https://www.identitytheft.gov/Steps (last accessed March 3, 2023).

[40] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

-- between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which has conducted studies regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See 2007 GAO Report, at p. 29.

121. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

122. There is a strong probability that the entirety of the stolen information has been dumped on the black market or will be dumped on the black market, meaning every Class Member, including Plaintiff, is at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

Plaintiff Taylor's Experience

123. Plaintiff Robert Taylor is, and at all times relevant to this complaint, a resident and citizen of the State of Connecticut.

124. Plaintiff Taylor is a consumer who is affiliated with Hatch Bank, a Customer of Fortra. Hatch Bank obtained Plaintiff's PII in order to provide him with its business

services. Fortra was provided with his PII by Hatch Bank, including but not limited to his Social Security number.

125. Around or after February 28, 2023, Plaintiff Taylor received the Notice of Data Breach letter, which indicated that Fortra had known about the Data Breach for nearly two months. The letter informed him that his critical PII was accessed by an unauthorized actor. The letter stated that the extracted information included his "name and Social Security number" but did not expand on whether additional information was stolen as well. (Taylor Notice of Data Breach Letter, attached as Exhibit A.)

126. Plaintiff Taylor is alarmed by the amount of his Personal Information that was stolen or accessed, and even more by the fact that his Social Security number was identified as among the breached data on Fortra's computer system.

127. Since the Data Breach, Plaintiff Taylor has been receiving a combination of around 7-8 spam calls, texts, and many spam emails per day. Prior to this time, he was receiving maybe one troublesome call and/or email per day.

128. Plaintiff Taylor is concerned that the spam calls and texts are being placed with the intent of obtaining more personal information from him and committing identity theft by way of a social engineering attack.

129. In response to Hatch's Notice of Data Breach, Plaintiff will be required to spend time dealing with the consequences of the Data Breach, which will continue to include time spent verifying the legitimacy of the Notice of Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts.

130. Plaintiff Taylor has already received an alert from an unauthorized charged

of $118.00 to his Chase Bank on February 20, 2023. He spent about an hour on the phone disputing this charge. He had to receive new bank cards as a result of this incident, which he believes is related to Fortra's Data Breach.

131. Plaintiff Taylor has been notified by his credit monitoring service that his information has been found on the dark web.

132. Plaintiff Taylor has taking efforts to mitigate his identity fraud risks, he has to continue utilizing a credit monitoring service through Norton Lifelock, and he has had to monitor his accounts more often since finding out about the Data Breach. He is even considering changing his phone number due to all of the inconvenience and nuisance the spam calls have caused him.

133. Immediately after receiving the Notice Letter, Plaintiff spent time discussing his options with a law firm and has started to check his financial accounts. He expects to spend a minimum of 7 hours per week in an effort to mitigate the damage that has been caused by Fortra.

134. Plaintiff is very careful about sharing PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

135. Plaintiff suffered actual injury and damages as a result of the Data Breach. Plaintiff would not have provided Hatch Bank—and in turn Fortra—with his PII had Fortra disclosed that it lacked data security practices adequate to safeguard PII.

136. Plaintiff suffered actual injury in the form of damages and diminution in the value of his PII—a form of intangible property entrusted to Fortra.

137. Plaintiff Taylor suffered lost time, annoyance, interference, and

inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy, especially his Social Security number.

138. Plaintiff Taylor reasonably believes that his Private Information may have already been sold by the cybercriminals. Had he been notified of Fortra's Data Breach in a timely manner, he would have been able to mitigate his injuries sooner.

139. Plaintiff Taylor has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen PII, especially his Social Security number, being placed in the hands of unauthorized third-parties and possibly criminals.

140. Plaintiff has a continuing interest in ensuring that his PII, which upon information and belief remains backed up and in Fortra's (and Hatch Bank's) possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

141. Plaintiff brings this action on behalf of themselves and on behalf of all other persons similarly situated ("the Class").

142. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All individuals whose Private Information was maintained on Fortra's computer systems and who was sent a notice of a data breach related to Fortra's 2023 Data Breach.

143. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are

Members of the judiciary to whom this case is assigned, their families and Members of their staff.

144. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

145. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class is believed to be in the thousands whose data was compromised in Data Breach.

146. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

A. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

B. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

C. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

D. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

E. Whether Defendant owed a duty to Class Members to safeguard their

Private Information;

F. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

G. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

H. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

I. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

J. Whether Defendant's conduct was negligent;

K. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and

L. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

147. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class member, was compromised in the Data Breach.

148. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating Class actions.

149. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' Private

Information was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

150. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

151. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

152. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- Whether Defendant owed a legal duty to Plaintiff and the Class to exercise

due care in collecting, storing, and safeguarding their Private Information;

- Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;
- Whether Defendant's failure to institute adequate protective security measures amounted to negligence;
- Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and
- Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

153. Finally, all members of the proposed Class are readily ascertainable. Defendant and/or its Customers have access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant or its Customers.

CAUSES OF ACTION

FIRST COUNT
Negligence
(On behalf of Plaintiff and All Class Members)

154. Plaintiff re-alleges and incorporates by reference the paragraphs above as if fully set forth herein.

155. Defendant gathered and stored the Private Information of Plaintiff and Class Members as part of the regular course of its business operations. Plaintiff and Class Members were entirely dependent on Defendant to use reasonable measures to safeguard

their Private Information and were vulnerable to the foreseeable harm described herein should Defendant fail to safeguard their Private Information.

156. By collecting and storing this data in its computer property, and sharing it, and using it for commercial gain, Defendant assumed a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a Data Breach.

157. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

158. Defendant had a duty to employ reasonable security measures under Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair ... practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

159. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

160. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures

and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

161. Defendant gathered and stored the Private Information of Plaintiff and Class Members as part of its business of providing its technology services to its Customers.

162. Defendant violated the FTC Act by failing to use reasonable measures to protect the Private Information of Plaintiff and Class Members and by not complying with applicable industry standards, as described herein.

163. Defendant breached its duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiff's and Class Members' Private Information, and by failing to provide prompt notice without reasonable delay.

164. Defendant's multiple failures to comply with applicable laws and regulations constitutes negligence per se.

165. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

166. Defendant had full knowledge of the sensitivity of the Private Information, the types of harm that Plaintiff and Class Members could and would suffer if the Private Information was wrongfully disclosed, and the importance of adequate security.

167. Plaintiff and Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class members had no ability to protect their Private Information that was in Defendant's possession.

168. Defendant was in a special relationship with Plaintiff and Class Members with respect to the hacked information because the aim of Defendant's data security measures was to benefit Plaintiff and Class Members by ensuring that their personal information would remain protected and secure. Only Defendant was in a position to ensure that its systems were sufficiently secure to protect Plaintiff's and Class Members' Private Information. The harm to Plaintiff and Class members from its exposure was highly foreseeable to Defendant.

169. Defendant owed Plaintiff and Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing their Private Information, including taking action to reasonably safeguard such data and providing notification to Plaintiff and the Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

170. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. See Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

171. Defendant had duties to protect and safeguard the Private Information of Plaintiff and the Class from being vulnerable to compromise by taking common-sense

precautions when dealing with sensitive Private Information. Additional duties that Defendant owed Plaintiff and the Class include:

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant' networks, systems, protocols, policies, procedures and practices to ensure that Plaintiff's and Class members' Private Information was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiff's and Class Members' Private Information in its possession by using reasonable and adequate security procedures and systems; and

c. To promptly notify Plaintiff and Class Members of any breach, security incident, unauthorized disclosure, or intrusion that affected or may have affected their Private Information.

172. Only Defendant was in a position to ensure that its systems and protocols were sufficient to protect the Private Information that had been entrusted to them.

173. Defendant breached its duties of care by failing to adequately protect Plaintiff's and Class Members' Private Information. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining, securing, safeguarding, protecting, and deleting the Private Information in its possession;

b. Failing to protect the Private Information in its possession using

reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store Private Information;

d. Failing to adequately train its employees to not store unencrypted Private Information in their personal files longer than absolutely necessary for the specific purpose that it was sent or received;

e. Failing to consistently enforce security policies aimed at protecting Plaintiff's and Class Members' Private Information;

f. Failing to mitigate the harm caused to Plaintiff and the Class Members;

g. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions; and

h. Failing to promptly notify Plaintiff and Class Members of the Data Breach that affected their Private Information.

174. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

175. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and Class Members have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

176. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the Private Information of Plaintiff and Class

Members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Private Information of Plaintiff and Class Members while it was within Defendant's possession and control.

177. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class Members, Defendant prevented Plaintiff and Class Members from taking meaningful, proactive steps to securing their Private Information and mitigating damages.

178. As a result of the Data Breach, Plaintiff and Class Members have spent time, effort, and money to mitigate the actual and potential impact of the Data Breach on their lives, including but not limited to, responding to the fraudulent use of the Private Information, and closely reviewing and monitoring bank accounts, credit reports, and statements sent from providers and their insurance companies.

179. Defendant's wrongful actions, inaction, and omissions constituted (and continue to constitute) common law negligence.

180. The damages Plaintiff and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

181. Plaintiff and the Class have suffered injury and are entitled to actual damages in amounts to be proven at trial.

SECOND COUNT
Breach of Implied Contract
(On Behalf of Plaintiff and All Class Members)

182. Plaintiff re-alleges and incorporates by the paragraphs above as if fully set forth herein.

183. Plaintiff and Class Members, through Defendant's Customers, were required to provide their PII as a condition of receiving business services provided by the Customers of Defendant.

184. Plaintiff and Class Members provided their PII in exchange for Defendant's Customer's services. In exchange for the PII, Defendant promised to Customers protect Plaintiff's and Class Members' PII from unauthorized disclosure.

185. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' Private Information would remain protected.

186. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the Private Information only under conditions that kept such information secure and confidential.

187. When Plaintiff and Class Members provided their Private Information to Customers of Defendant as a condition of relationship, they entered into implied contracts with the Customers and Defendant pursuant to which Defendant agreed to reasonably protect such information.

188. Customers required Class Members to provide their Private Information, which was to be protected on their behalf as part of Defendant's regular business practices.

189. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Customers' and Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

190. Plaintiff and Class Members would not have entrusted their Private Information to Customers or Defendant in the absence of the implied contract between them to keep their information reasonably secure.

191. Plaintiff and Class Members would not have entrusted their Private Information to Customers of Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

192. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts.

193. Defendant breached its implied contracts with its Customers made on behalf of the Class Members by failing to safeguard and protect their Private Information.

194. As a direct and proximate result of Defendant's breaches of the implied contracts, Class Members sustained damages as alleged herein.

195. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

196. Plaintiff and Class Members are also entitled to nominal damages for the breach of implied contract.

197. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate long term credit monitoring to all Class Members for a period longer than the grossly inadequate time currently offered.

THIRD COUNT
Unjust Enrichment
(On Behalf of Plaintiff and All Class Members)

198. Plaintiff re-alleges and incorporates by reference the paragraphs above as if fully set forth herein.

199. Plaintiff and Class Members conferred a monetary benefit on Defendant through its Customers in the form of the provision of their Private Information and Defendant would be unable to engage in its regular course of business without that Private Information.

200. Defendant appreciated that a monetary benefit was being conferred upon it by its Customers on behalf of Plaintiff and Class Members and accepted that monetary benefit.

201. However, acceptance of the benefit under the facts and circumstances outlined above make it inequitable for Defendant to retain that benefit without payment of

the value thereof. Specifically, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite data security.

202. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures.

203. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

204. If Plaintiff and Class Members knew that Defendant had not secured their Private Information, they would not have agreed to provide their Private Information to Defendant through its Customers.

205. Plaintiff and Class Members have no adequate remedy at law.

206. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with

effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

207. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

208. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

FOURTH COUNT
Declaratory Judgment
(On Behalf of Plaintiff and All Class Members)

209. Plaintiff re-alleges and incorporates by reference the paragraphs above as if fully set forth herein.

210. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described

in this Complaint.

211. An actual controversy has arisen in the wake of the Defendant data breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' Private Information and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class members from further data breaches that compromise their Private Information.

212. Plaintiff allege that Defendant's data security measures remain inadequate. Plaintiff will continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

213. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

214. a. Defendant continues to owe a legal duty to secure consumers' Private Information and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes;

215. b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Private Information.

216. The Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect consumers' Private Information.

217. If an injunction is not issued, Plaintiff and Class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach

at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiff and class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

218. The hardship to Plaintiff and Class members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another massive data breach occurs at Defendant, Plaintiff and class members will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

219. Issuance of the requested injunction will not do a disservice to the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiffs and the millions of consumers whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and his counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse

and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures of its Data Breach to Plaintiff and Class Members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. For declaratory relief as requested;

F. Ordering Defendant to pay for lifetime credit monitoring services for Plaintiff and the Class;

G. For an award of actual damages, compensatory damages, and statutory damages, in an amount to be determined, as allowable by law;

H. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

I. Pre- and post-judgment interest on any amounts awarded; and

J. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Respectfully submitted,

Dated: March 6, 2023

/s/ Brian C. Gudmundson

Brian C. Gudmundson, MN Bar No. 336695
Michael J. Laird, MN Bar No. 398436
Rachel K. Tack, MN Bar No. 399529
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
brian.gudmundson@zimmreed.com
michael.laird@zimmreed.com
rachel.tack@zimmreed.com

Gary E. Mason*
Danielle L. Perry*
Lisa A. White*
MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015
Telephone: (202) 429-2290
gmason@masonllp.com
dperry@masonllp.com
lwhite@masonllp.com

Attorneys for Plaintiff
**Pro hac vice applications to be filed*